contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Perforce Puppet Enterprise exploited

CVE-2026-115731 · on CISA's exploited list since 17 November 2026

Analysis Report

If you run Puppet Enterprise, upgrade to 2023.8.13, 2025.12.1 or 2026.0.1 and restart puppet server before CISA's date of 1 December 2026. First find out whether you run it and which version. If you …

PREPARED BY	NamiQ	DATE	18 November 2026
FACTS AS OF	18 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	STATUS	On CISA's exploited list; due 1 December 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/perforce-puppet-enterprise-cve-2026-115731

The bottom line

> *If you run Puppet Enterprise, upgrade to 2023.8.13, 2025.12.1 or 2026.0.1 and restart puppet server before CISA's date of 1 December 2026. First find out whether you run it and which version. If you do not run it, you can stop reading.*

At a glance

Fact	Detail
Product	Perforce Puppet Enterprise (CVE-2026-115731)
Severity	Critical: 9.9 (CVSS 3.1)
CISA	On its exploited list since 17 November 2026. Deadline for US federal agencies: 1 December 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 18 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Puppet Enterprise 2023.8.13, 2025.12.1 or 2026.0.1 (these bundle puppet-agent 8.22.2 or 9.1.3), then restart puppet server. The record says so; no vendor page was read.
Who looks first	Whoever runs Puppet Enterprise, mainly the Puppet Server, on 2023.8.0 up to 2023.8.13, 2025.0.0 up to 2025.12.1, or 2026.0.0 up to 2026.0.1. Check the signing setup too.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Puppet Enterprise, or does your IT provider run it for you?	Nothing to do for this CVE.	Check the version (next question).
Does your certificate authority sign agent requests automatically?	An outsider cannot get a certificate that way, but any holder of one can still exploit it. Upgrade.	Treat it as reachable by anyone who can reach the server. Upgrade first.

Can untrusted machines reach the Puppet Server over the network?	Exposure is lower. The upgrade is still needed.	Restrict access to known machines while you upgrade.

What it is

A machine holding any certificate signed by the Puppet certificate authority can run its own code on the Puppet Server, as the server's service user, by sending a crafted report. If the authority signs requests automatically without strong checks, an outsider can get such a certificate.

Why it matters

Our reading is that the attacker needs a certificate, not a password. The record says automatic signing can hand one to an outsider over the network. So the weak point is how requests are signed, as much as the version. The record also does not say what the service user can reach, so assume the server itself is fully compromised until shown otherwise.

Things people will get wrong

- "We sign requests by hand, so we are safe." Not by itself. The record says any client with a CA-signed agent certificate can exploit it. Automatic signing only makes a certificate easier for an outsider to get.
- "Upgrading the package is enough." The record says to restart puppet server so the fixed code is loaded.
- "It needs a login to the server." No. The record says a valid agent certificate is enough, sent in a PUT request carrying a crafted report.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the versions you run

- List every Puppet Enterprise server and note its version. The ranges in the record are by Puppet Enterprise release.
- Ask your provider if they run one on your behalf.

```
puppet --version
puppetserver --version
```

Step 2: Check how requests are signed

- Find out whether the certificate authority signs agent requests automatically. The record says that is what lets an outsider get a certificate.
- Switch to manual or strongly verified signing if you can.

Step 3: Reduce who can reach the server

- Limit network access to the Puppet Server to the machines that need it, until the upgrade is done.
- Review certificates signed recently and revoke any you do not recognise.

Step 4: Upgrade and restart

- Move to 2023.8.13, 2025.12.1 or 2026.0.1, as fits your branch, then restart puppet server so the fixed code is loaded.
- Re-run the version check and keep the output as proof.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello. CISA lists CVE-2026-115731, a flaw in Puppet Enterprise that lets a holder of any CA-signed agent certificate run code on the Puppet Server. Please tell us whether we run Puppet Enterprise, where, and which version. The record gives the fixed releases as 2023.8.13, 2025.12.1 and 2026.0.1, with a restart of puppet server afterwards. Please also tell us whether certificate requests are signed automatically. CISA's date is 1 December 2026. Please confirm in writing the version and that the fix is in place by 25 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- New agent certificates signed recently that you did not expect, or reports arriving from machines you do not manage.
- Unusual processes or new files created by the Puppet Server's service user.
- PUT requests carrying reports from unfamiliar clients in the server's logs.

The weakness behind it

The record classes this as CWE-502 (Deserialization of Untrusted Data) and CWE-94 (Improper Control of Generation of Code).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The record describes an unauthenticated network attacker reaching the server and sending a request. That would likely amount to exploiting an exposed service.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The flaw gives arbitrary code execution as the service user, which would typically let an attacker run commands on the server.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Perforce Puppet Enterprise contains a deserialization of untrusted data vulnerability in Puppet's report-processing code that allows a client with any CA-signed agent certificate to execute arbitrary code on the Puppet Server as the service user by submitting a report containing a crafted rich-data type through a PUT request. If the certificate authority automatically signs requests without strong verification, an unauthenticated network attacker can obtain a valid certificate and exploit the vulnerability.*

The CVE record, published by Perforce on 3 November 2026:

> *Deserialization of untrusted data in the report-processing code of Puppet, as used by Puppet Server, in the affected releases, allows a client that holds any CA-signed agent certificate to execute arbitrary code on the Puppet Server as its service user by submitting a report containing a crafted rich-data type via PUT request. Where the certificate authority autosigns requests without strong verification, an unauthenticated network attacker can obtain such a certificate.*

Versions of Perforce Puppet Enterprise the record lists as affected:

- 2023.8.0 up to, but not including, 2023.8.13
- 2025.0.0 up to, but not including, 2025.12.1
- 2026.0.0 up to, but not including, 2026.0.1

It lists these as unaffected:

- 2023.8.13
- 2025.12.1
- 2026.0.1

The affected ranges end before 2023.8.13, 2025.12.1, 2026.0.1. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

What the record says to do about it, in the vendor's words:

> *Upgrade to a release that bundles puppet-agent 8.22.2 or 9.1.3 (Puppet Enterprise 2023.8.13, 2025.12.1, or 2026.0.1) and restart puppet server so the fixed code is loaded.*

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-115731
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-115731
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- No vendor page could be read, so other flaws fixed in these releases and any workaround are not known here.
- Whether the service user has wide access on the server is not stated.
- Which kinds of automatic signing count as 'without strong verification' is not defined in the record.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 18 November 2026; the vendor's advisory wins where it differs.

- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-115731: score 9.4, `CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
3 November 2026	CVE record published by Perforce.
17 November 2026	CISA added it to its list of exploited vulnerabilities.
1 December 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe

Affected version, automatic signing on, server reachable from networks you do not control	High	Within CISA's window; start now
Affected version, signing is manual, but many machines hold valid certificates	High	Within CISA's window
Affected version, server reachable only from a small, trusted set of machines	Medium	This week, and within CISA's window
Version already at 2023.8.13, 2025.12.1 or 2026.0.1 or later, but server not restarted since upgrade	Medium	At the next safe moment, soon
You do not run Puppet Enterprise	None	None for this CVE

Appendix 4. Definition of done

- Every Perforce Puppet Enterprise you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-115731: https://www.cve.org/CVERecord?id=CVE-2026-115731
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: portal.perforce.com: https://portal.perforce.com/s/cve/a91Qi000003IaHpIAK/report-deserialization-code-execution